REMARKS

This Amendment is fully responsive to the non-final Office Action dated November 1, 2007 issued in connection with the above-identified application. Claims 3-16, 18-34, 49 and 69-76 are all the claims presently pending in the application. With this Amendment, claims 49 and 69-75 have been amended. No new matter has been introduced by the amendments made to the claims. Favorable reconsideration is respectfully requested.

In the Office Action, claims 3, 7, 10, 11, 13-15, 18, 19, 23, 28, 29, 49 and 69-74 have been rejected under 35 USC 103(a) as being unpatentable over Yang et al. ("Reliable Group Rekeying: A Performance Analysis," hereafter "Yang") in view of Ray et al. (US Publication No. 2003/0112977, hereafter "Ray"). Claims 3-6 and 69 have been rejected under 35 USC 103(a) as being unpatentable over Wong et al. ("Keystone: A Group Key Management Service," hereafter "Wong") in view of Yang, and further in view of Ray. And, claims 8 and 9 have been rejected under 35 USC 103(a) as being unpatentable over Yang in view Ray, and further in view of Steiner et al. ("Cliques: A New Approach to Group Key Arrangement," hereafter "Steiner").

Additionally, claims 3, 12 and 69 have been rejected as being unpatentable over Paolo (UK Patent No. 2343025, hereafter "Paolo") in view of Yang, and further in view of Ray. Claim 16 has been rejected as being unpatentable over Yang in view of Ray, and further in view of Canetti et al. ("Multicast Security: A Taxonomy and Some Efficient Construction," hereafter "Canetti"). Claims 3, 20-22, 24-27, 34 and 69 have been rejected under 35 USC 103(a) as being unpatentable over Yevgeny (UK 2353682, hereafter "Yevgeny") in view of Yang, and further in view of Ray. Finally, claims 3, 30-33 and 69 were rejected as being unpatentable over Huang et al. ("Group Leader Election Under-State Routing," hereafter "Huang") in view of Yang, and further in view of Ray.

The Applicants have amended independent claims 49 and 69-75 to further distinguish the present invention over the cited prior art. As amended, independent claims 49 and 69-75 now more clearly point out the novel use of "common secret information" and "valid period information" by a group management device for managing the use of content in a content management system (see e.g., Applicants'

disclosure, page 4 and page 66). For example, claim 49 has been amended to recite the following:

"A member device that uses a content after registering in a group managed by a group managing device included in a group management system composed of a plurality of member devices including the member device and the group management device, the member device comprising:...

a receiving unit operable to be authenticated by the group management device, and to receive from the group management device, common secret information and valid period information, the common secret information being unique to the group and common among a plurality of member devices registered in the group, and the valid period information showing a valid period of use of the common secret information, and the valid period being unique to the member device..." (Emphasis added).

The features emphasized above in independent claim 49 are similarly recited in independent claims 69-75. Specifically, claim 69 is directed to a group management device; claim 70 is directed to a group management system; claim 71 is directed to a group management method; claim 72 is directed to a recording medium storing a program used by a group management device; claim 73 is directed to a control method used by a member device; claim 74 is directed to a recording medium storing a program used in a member device; and claim 75 is directed to a group management device. Claims 69-75 all include the novel use of "common secret information" and "valid period information" noted above in claim 49.

The present invention, as recited in claims 49 and 69-75, is distinguishable over the cited prior art in that the common secret information is unique to a group and common among a plurality of member devices registered in the group. The valid period information indicates a valid period of use of the common secret information, and the valid period is unique to each member device. The use of both types of information noted above allows for greater flexibility for accessing content, while preventing any member device in a group from accessing content for an indefinite period of time.

Additionally, the present invention (as recited in claims 49 and 69-75) provides the advantage that a group management device can reduce the registered number of member devices when a valid period set for the member device ends, even if a member

device is not connected on-line with the group management device. Moreover, it is possible to reduce the registered number of member devices by performing withdrawal processing in a member device based on a valid period individually set for the member device, without receiving a voluntary withdrawal request from the member device.

The Applicants maintain that the above features and advantages of the present invention are not disclosed or suggested by the cited prior art, individually or in combination.

Yang discloses a group rekeying method. As described in Yang, when a group key that is common in a group is updated, it is possible to reduce the traffic required for updating the group key by performing batch processing of join/leave requests received from terminals during a valid period of the group key (rekey interval). In Yang, the terminals are assigned to leaf nodes in a tree structure by using a binary tree structure. When a terminal leaves the group, a newly joined terminal is assigned to the"empty" leaf node. The terminals are assigned to leaf nodes so as not to destroy the tree structure, and to reduce the traffic required for updating the group key.

In the Office Action, the Examiner relies on section"2.3 Periodic batch rekeying" and section "2.4 Batch rekeying algorithms" in Yang for disclosing use of the claimed "valid period information." However, Yang merely discloses that the periodic batch rekeying is performed to increase efficiency. Additionally, Yang clearly discloses that "a valid period of a common group key is distributed to group members." In other words, the valid period for use of the common group key is not unique to each member device, but is provided to all group members. The Examiner also appears to have acknowledge this point by the Applicants in the Office Action (see e.g., pg. 8).

Thus, Yang clearly fails to discloses or suggests at least the use of common secret information unique to a group and common among a plurality of member devices registered in the group, and valid period information showing a valid period of use of the common secret information, wherein the valid period is unique to the member device, as in claims 49 and 69-75 (as amended).

Ray discloses a method for securely communicating data in a mobile communications network. In the Office Action, the Examiner relies on Ray for disclosing the use of a session key and a valid period for using common secret information that is unique to a

member device (see e.g.,¶ [0013] and ¶ [0039]). However, the Applicants maintain that there is no motivation to combine the teachings of Ray with Yang. Additionally, even if the combination is made, the combination still would not teach or suggest all the features recited in claims in claim 49 and 69-75 (as amended).

Ray, at ¶ [0013], discloses that a mobile authentication center assigns a valid time period for a generated session key that is used by a wireless device. A more detailed description of the use of the session key in Ray is described in ¶ [0039]. As described in ¶ [0039], the mobile authentication center generates a session key that is unique to a device, and further assigns a time period for which the assigned session key may be used.

As noted above, the valid time period described in Ray is a valid period for use of the unique session key (i.e., unique to a device) within a session. The valid time period is not related to a time period for using a common group key that is shared among member devices of a group. In fact, the only group key disclosed is Ray (e.g., ¶ [0037]) is described "as being randomly generated from the session key." Therefore, similar to the session key, the group key described in Ray is also unique to a device (i.e., not shared among devices in a group). Moreover, the valid time period described in Ray is not unique to a device, but appears to be unique to a session for using the session key.

Therefore, the method in Ray does not exhibit the following advantages achieved by the present invention: 1) a certain number of member devices that share a common group key with each other; and 2) a valid period individually set for each member device registered in the group for using the common group key.

In summary, Yang discloses use of a common group key, but fails to disclose a valid period for use of the common group key that is unique to each device in the group. Additionally, Ray discloses the use of a unique session key, a unique group key; and a valid period for using the unique session key. To this end, Ray actually teaches away from use of a valid period for using a common group key, as disclosed in Yang.

Additionally, Yang in view of Ray still fail to discloses or suggests at least the use of common secret information unique to a group and common among a plurality of member devices registered in the group; and valid period information showing a valid period of use of the common secret information, wherein the valid period is unique to

the member device, as in claims 49 and 69-75 (as amended).

Moreover, after a detailed review of Steiner, Paolo, Canetti, Yevgeny and Huang, the references fail to overcome the deficiencies noted above in Yang in view of Ray.

Accordingly, no obvious combination of the cited prior art would result in, or otherwise render obvious, the features of independent claims 49 and 69-75 (as amended). Likewise, no combination of the cited prior art would result in or otherwise render obvious claims 3-16, 18-34 and 76, based at least on their respective dependency from independent claims 69 and 75.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance, and the Examiner is requested to pass the case to issue. If the Examiner should have any comments or suggestions to help speed the prosecution of this application, the Examiner is requested to contact Applicants' undersigned representative.

Respectfully submitted,

Natsume MATSUZAKI et al.

By: 

Mark D. Pratt
Registration No. 45,794
Attorney for Applicants

MDP(MSH)/ats
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 31, 2008